COMNAVRESFOR INSTRUCTION 5300.5A

From: Commander, Navy Reserve Force

Subj: INFORMATION TECHNOLOGY AND NAVY MARINE CORPS INTRANET GUIDANCE

Ref: (a) CIO memo of 25 Jan 13 MFD Guidance
    (b) DoD 5000.7-R, Joint Ethics Regulation, November 1993
    (c) SECNAV 192027Z Aug 10
    (d) SECNAV 192031Z Aug 10
    (e) SECNAVINST 5239.3B
    (f) SECNAVINST 5210.8D
    (g) DON CIO 032009Z Oct 08
    (h) 44 U.S.C. 3541
    (i) SECNAV M-5510.30, Department of the Navy (DON) Personnel Security Program
    (j) SECNAV M-5210.1, Records Management Manual
    (k) COMNAVNETWARCOM ltr 5239 Ser ODAA/1001 of 9 May 11
    (l) DON CIO 161108Z Jul 05
    (m) DoD Instruction 8500.2 of 6 February 03

Encl: (1) Administrative Information Technology Procedures for the Navy Reserve Force

1. Purpose. The purpose of this instruction is to promulgate guidance for Navy Reserve Information Technology (IT) usage to meet claimancy-wide requirements. These requirements maximize efficiency and cost effectiveness for Enterprise Architecture (EA), Information Assurance (IA), security, management, distribution, administration and user responsibilities, per references (a) through (m), within a limited Navy Marine Corps Intranet (NMCI)/Continuity of Service Contract (CoSC) budget. This instruction is a complete revision and should be reviewed in its entirety. Furthermore, this guidance will be revised accordingly to reflect the implementation of the forthcoming Next Generation Enterprise Network (NGEN) services contract in FY-15.

2. Cancellation. COMNAVRESFORINST 5300.5.
   COMNAVRESFORINST 5233.1.
3. **Scope.** This instruction provides policy for the administration of the Navy Reserve Force's IT investments and IT services portfolio.

4. **Forms.** The following form is available under the forms section on the Navy Reserve Website:

NAVRES 5300/3 (3-14), Request for New Site or Community of Interest Space.

[Signature]

R. R. BRAUN
Vice Admiral, U.S. Navy

Distribution:
Electronic copy via COMNAVRESFOR Web site
https://www.navyreserve.navy.mil
ADMINISTRATIVE
INFORMATION TECHNOLOGY
PROCEDURES FOR THE
NAVY RESERVE FORCE

Enclosure (1)
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Subject</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHAPTER 1 NAVY RESERVE GENERAL INFORMATION TECHNOLOGY OPERATIONS</td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Action</td>
<td>1</td>
</tr>
<tr>
<td>Budget Guidelines</td>
<td>1</td>
</tr>
<tr>
<td>Ordering Guidelines</td>
<td>1</td>
</tr>
<tr>
<td>Laptops</td>
<td>2</td>
</tr>
<tr>
<td>MobiKEY</td>
<td>2</td>
</tr>
<tr>
<td>Mobile Unclassified Remote Access Service Group Category</td>
<td>3</td>
</tr>
<tr>
<td>Secret Internet Protocol Router Network</td>
<td>3</td>
</tr>
<tr>
<td>Blackberry - Research in Motion</td>
<td>3</td>
</tr>
<tr>
<td>Cell Phones</td>
<td>4</td>
</tr>
<tr>
<td>Personal Digital Assistant/Smart Phones/Tablet</td>
<td>4</td>
</tr>
<tr>
<td>Information Technology Inventory</td>
<td>4</td>
</tr>
<tr>
<td>Information Technology Pre-Invoices</td>
<td>4</td>
</tr>
<tr>
<td>Procurement Requests</td>
<td>4</td>
</tr>
<tr>
<td>EMAIL Storage</td>
<td>4</td>
</tr>
<tr>
<td>Printer Distribution</td>
<td>5</td>
</tr>
<tr>
<td>Reserve Flag Officer Information Technology Support</td>
<td>6</td>
</tr>
<tr>
<td>Account Management</td>
<td>6</td>
</tr>
<tr>
<td>Message Traffic</td>
<td>6</td>
</tr>
</tbody>
</table>

Enclosure (1)
TABLE OF CONTENTS (CONT'D)

<table>
<thead>
<tr>
<th>Subject</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Definitions</td>
<td>7</td>
</tr>
<tr>
<td>Examples of different accounts</td>
<td>7</td>
</tr>
<tr>
<td>Figure 1-1 Navy Marine Corps Intranet/Continuity of Service Contract Ordering Guidelines</td>
<td>9</td>
</tr>
<tr>
<td>CHAPTER 2 SOFTWARE AND USER PERMISSIONS</td>
<td>10</td>
</tr>
<tr>
<td>Common Access Card Enabled Sites</td>
<td>10</td>
</tr>
<tr>
<td>SharePoint</td>
<td>10</td>
</tr>
<tr>
<td>Site Troubleshooting</td>
<td>11</td>
</tr>
<tr>
<td>Site Permission Management</td>
<td>11</td>
</tr>
<tr>
<td>SharePoint Training</td>
<td>11</td>
</tr>
<tr>
<td>User Profile Synchronization</td>
<td>11</td>
</tr>
<tr>
<td>Linking .COM Sites</td>
<td>12</td>
</tr>
<tr>
<td>Commercial EMAIL</td>
<td>12</td>
</tr>
<tr>
<td>Defense Connect Online</td>
<td>14</td>
</tr>
<tr>
<td>CHAPTER 3 INFORMATION TECHNOLOGY SUPPORT AND VERIFICATION</td>
<td>16</td>
</tr>
<tr>
<td>Contingency of Operations Plan</td>
<td>16</td>
</tr>
<tr>
<td>Remote Site Information Technology Support</td>
<td>16</td>
</tr>
<tr>
<td>System Authorization Access Forms</td>
<td>16</td>
</tr>
<tr>
<td>CHAPTER 4 NAVY OPERATIONAL SUPPORT CENTER WI-FI USAGE PROCEDURES AND USER RESPONSIBILITIES</td>
<td>17</td>
</tr>
<tr>
<td>General</td>
<td>17</td>
</tr>
<tr>
<td>Scope</td>
<td>17</td>
</tr>
</tbody>
</table>

Enclosure (1)
<table>
<thead>
<tr>
<th>Subject</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bring Your Own Device</td>
<td>17</td>
</tr>
<tr>
<td>Responsibilities</td>
<td>17</td>
</tr>
<tr>
<td>Trouble Shooting Personal Devices</td>
<td>20</td>
</tr>
<tr>
<td>Enforcement</td>
<td>21</td>
</tr>
<tr>
<td>Figure 4-1</td>
<td></td>
</tr>
<tr>
<td>Wi-Fi User Device Initial Setup Checklist</td>
<td>22</td>
</tr>
<tr>
<td>APPENDIX A</td>
<td></td>
</tr>
<tr>
<td>ACRONYMS AND DEFINITIONS</td>
<td>23</td>
</tr>
<tr>
<td>APPENDIX B</td>
<td></td>
</tr>
<tr>
<td>FORMS AND UNIFORM RESOURCE LOCATOR</td>
<td>25</td>
</tr>
<tr>
<td>AVAILABILITY</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 1

NAVY RESERVE INFORMATION TECHNOLOGY OPERATIONS

1. Introduction. Navy Regional Reserve Component Commands (RCCs) will be responsible for the administration of every COMNAVRESFOR command within their geographic region for all matters concerning NMCI/CoSC. Navy Air Facility Washington, Office of the Chief of Navy Reserve Staff Detachment, Information Dominance Corps Reserve Command, Navy Expeditionary Logistics Support Group, Navy Air Logistics Office and Navy Reserve Professional Development Center will be responsible for managing NMCI/CoSC in their cognizant areas within COMNAVRESFOR.

2. Action. All commands attached to Commander, Navy Reserve Force (COMNAVRESFOR) must adhere to the following updated baseline ordering model to meet computing and connectivity requirements. Direct all requests for explanation of this guidance to the Reserve Force NMCI/CoSC IT Operations Manager (N63).

3. Budget Guidelines. COMNAVRESFOR manages the claimant-wide NMCI/CoSC budget. Commands may make changes to their NMCI/CoSC task order, but additions must be authorized by COMNAVRESFOR N63 to ensure the change remains within the authorized budget. All conditions of this instruction are dependent on the availability of funding and requested assets.

4. Ordering Guidelines. The ordering guidelines are a framework for assisting the RCCs in calculating the suggested asset allowance for each type of command in their area of responsibility. Figure 1-1 provides amplifying information.

   a. Echelon II, III, IV, V:

      (1) One NMCI/CoSC seat for each Full Time Support (FTS).

      (2) One NMCI/CoSC administrative seat for the command.

      (3) One NMCI/CoSC training seat for every 13 Selected Reserve (SELRES) Sailors.

Enclosure (1)
b. Commander, Naval Air Force Reserve Command Aviation Supply Departments (ASD)/Fleet Readiness Commands (FRC):

(1) One NMCI/CoSC seat for each FTS officer.

(2) Two NMCI/CoSC seats for every three FTS enlisted.

(3) One NMCI/CoSC training seat for every 18 SELRES.

c. Navy Reserve Echelon VI Units:

(1) One NMCI/CoSC Laptop, desktop or a Hosted Virtual Device (HVD) for the Unit Commanding Officer (CO).

(2) One NMCI/CoSC administrative seat. This seat can be either a portable or fixed seat.

(3) Additional seats can be requested via the Echelon III/IV/V chain of command to support unit specific requirements and/or mobilization readiness.

5. Laptops

a. Echelon II and III: NOO, NOOB, N01, N01B, N00C, N00A, Special Assistants, Flag Assistants and all Deputy Chief of Staffs (DCOSs) are authorized a laptop. Exceptions must be approved by the Chief of Staff (COS) or Chief Staff Officer (CSO).

b. Echelon IV: Commander, CSO and Senior Enlisted Advisor are authorized a dedicated desktop or laptop, within budget guidelines. Exceptions must be approved by the RCC COS/CSO.

c. Echelon V and VI: COs are authorized a dedicated desktop or laptop, within budget guidelines. Exceptions must be approved by the RCC CSO.

d. Section 9 addresses issuance of laptop computers with BlackBerry devices.

6. MobiKEY

a. Echelon II, III, IV and V personnel who are authorized a dedicated desktop may also be authorized a MobiKEY.
b. Echelon VI Unit COs who have a dedicated desktop may choose a MobiKEY instead of a BlackBerry or laptop with aircard or Wi-Fi card.

7. Mobile Unclassified Remote Access Service (Air Cards/Wi-Fi). The appropriate COS/CSO may authorize NMCI/CoSC certified air cards or Wi-Fi cards for use with NMCI/CoSC laptops. Air Cards/Wi-Fi can only be issued by COMNAVRESFOR N6 and are not authorized to be funded with local operating target.

8. Secret Internet Protocol Router Network. A minimum of one Secret Internet Protocol Router network (SIPRNET) seat is authorized for each Echelon IV and V command. This requires a secure enclave to be built and certified prior to installation of SIPRNET seats. Navy Operational Support Centers (NAVOPSPTCENs) are to maintain organic SIPRNET capability, as pre-deployment requirements leverage SIPRNET connectivity. All sites require 24/7 access to SIPRNET. If a site does not have access, then steps shall be taken to meet SIPR requirements. If a site is unable to meet these requirements but has the ability to procure access via another Department of Defence (DoD) facility, requirements can be satisfied with a Memorandum of Agreement (MOA). COMNAVRESFOR does not support removal of SIPRNET at sites in either of the following conditions:

a. The CO would prefer to leverage a MOA with a nearby DOD facility.

b. The CO does not want the responsibility of operating a SIPRNET computer or Secure Terminal Equipment.

9. BlackBerry - Research in Motion. BlackBerrys are the only portable devices authorized for use with the NMCI/CoSC contract. Additionally, a cellular data plan must be on the NMCI/CoSC Certified Device List. BlackBerry devices must be authorized and ordered by COMNAVRESFOR N63 against the authorized funding line.

a. Echelons II, III, IV and V personnel authorized a NMCI laptop may be authorized a BlackBerry. If a BlackBerry is chosen, a desktop computer will be issued instead of a laptop. Waivers can be granted by the appropriate COS/CSO.

b. Echelon VI Commissioned Unit COs may choose a BlackBerry instead of a computer. BlackBerry users must have a BlackBerry Common Access Card (CAC) reader to sign and or access encrypted e-mail.

Enclosure (1)
An available desktop computer must also be identified to synchronize the BlackBerry.

10. Cell Phones. Stand-alone cell phone services will be procured through one of the Naval Supply Fleet Logistics Center (FLC) San Diego authorized vendors only, using the authorized funding line. They may not be purchased from retail stores or other non-FLC channels or funds. Stand-alone cell phones may be purchased with voice and text services only. Data plans are not authorized.

11. Personal Digital Assistants/Smart Phones/Tablets. Personal Digital Assistants (PDAs), Smart Phones and Tablets are not available through the NMCI/CoSC contract. This includes devices which use Apple iOS, Google Android, Microsoft Mobile Windows, etc. These devices are neither approved for purchase outside of FLC channels, nor are they on the NMCI/CoSC Certified Device List. Therefore, they cannot be connected to NMCI/CoSC EMAIL service.

12. IT Inventory. Inventory of NMCI and other IT assets to include NMCI computers, laptops, air cards, MobiKEYs, Wi-Fi cards and BlackBerrys will be required annually and as scheduled by COMNAVRESFOR. Corrections to errors will be made in the NMCI Enterprise Tool (NET) as the sole authority of that data. Personnel completing IT Inventories and working with NET are to complete NET Training via the Uniform Resource Locator (URL): https://net.ahf.nmci.navy.mil/default.aspx.

13. IT Pre-Invoices. Customer Technical Representatives (CTR) shall ensure NMCI pre-invoices are validated monthly and as required utilizing eMarketplace.

14. Procurement Requests. All non-NMCI IT purchases, regardless of cost, are required to be submitted and approved through Information Technology Procurement Requests via Navy Information Dominance Approval System (NAV-IDAS). Personnel completing procurement requests and working with NAV-IDAS are to complete training via the following URL: https://navidas.navy.mil/training.html.

15. EMAIL Storage. EMAIL accounts are set by NMCI at a limit of 100MB. Additional NMCI/CoSC EMAIL storage and Data Seat Back-up and Recovery can be authorized by the regional Deputy Customer Technical Representative. Users are encouraged to create local .pst files to mitigate EMAIL storage issues when exceeding NMCI limits.
16. **Printer Distribution**

   a. Per reference (a), Commander, Navy Reserve Forces Command (COMNAVRESFORCOM) is limiting the procurement of single function print/scan/fax/copy devices. Multi-Functional Devices (MFDs) are the only method for printing, scanning, faxing and photocopying. This policy applies to all echelons of COMNAVRESFOR. The intent is to attain an optimal mix of capability to meet requirements as applied to unclassified and classified local and networked devices for new and technical refresh requirements. Fax capability will be included in MFDs as appropriate certification for telecommunications capability becomes available.

   b. **MFD Implementation Plan:**

   (1) New requirements for office printing, scanning and photocopying of unclassified documents shall be met by purchasing a MFD.

   (2) New requirements for office printing, scanning and photocopying of classified documents shall be met to the maximum extent practicable with MFDs while ensuring compliance with applicable security rules and regulations.

   (3) The MFD shall include a Fax capability that shall be enabled when the appropriate certification is available.

   (4) MFD devices from NMCI Contract Line Item Number (CLIN) 23 list are the preferred devices.

   (5) Existing single function devices shall continue to operate until service life is met.

   (6) Single function devices that fail will be replaced by a general office use MFD. Consideration for purchase of a single use device must meet the waiver/cost benefit requirements of the MFD policy.

   (7) Single function devices in the same office work area as a MFD shall be removed from service to the maximum extent practical to conserve resources.

Enclosure (1)
17. **Reserve Flag Officer IT Support.** COMNAVRESFOR IT Help Desk will procure, deploy and provide equipment and customer service, to include follow-up on NMCI/CoSC trouble tickets to all Reserve Flag Officers.

18. **Account Management**

   a. Active NMCI/CoSC unclassified accounts are required for all members of the Navy Reserve (including FTS, SELRES and Voluntary Training Unit members. A profile for every account will be established in NMCI/CoSC NET which will allow COMNAVRESFOR to maintain an accurate total of the number of accounts assigned to COMNAVRESFOR at anytime. Examples of various situations affecting reserve personnel and the state of their accounts are included in Figure 1-1.

   b. An account must be deactivated upon a member’s death, retirement or separation from the Navy. The Echelon IV and V deputy/assistant CTRs are responsible for checking 90 days after deactivation or per the annual account clean to ensure the action has been completed. The respective CTR may choose temporary suspending or permanent deactivation. Temporarily suspend an account if the service member may join the Navy in another capacity (FTS to SELRES or contractor, etc). The account should be permanently deactivated if the member has not transferred after the 90 day period has expired.

   c. The existing account should be reactivated for members transferring from a non-NMCI/CoSC command and for those returning to a command with NMCI/CoSC access. New accounts should not be created if an account already exists in the active directory.

   d. All accounts will be verified monthly in NET or via automated reports provided by COMNAVRESFOR. Verification will be consolidated at Echelon IV for subordinate activities and appropriate action taken for accounts that are not in use or no longer required. Additionally, all accounts will be entered into NET including previously created accounts.

19. **Message Traffic.** All commands will maintain their own Plain Language Address and the ability to transmit and receive message traffic.
20. Account Definitions

a. Active Account: Provides the member access to the NMCI/CoSC Network, 100MB EMAIL storage space and 700MB of personal storage space (H: Drive).

b. Deactivated Account: End of service for an NMCI/CoSC Account. This occurs when all NMCI/CoSC services are discontinued. The account will be moved out of the local Command Organizational Unit (OU) structure, attributes will be reduced to digital identity and flat name space and associated data will be compressed and moved to a permanent data storage facility. Do not deactivate the accounts of members who are transferring between commands that are serviced by NMCI/CoSC.

c. Disabled/Suspend Account: An account that is not accessible and all EMAIL is rejected. This type of account would be used by the Information System Security Manager to lock an account.

d. Functional Account: Active accounts established for specific duties as approved by by Echelon II, III or IV Information Assurance Manager (IAM). Example: Command Duty Officers and watch standing roles.

e. Reactivated Account: A deactivated account reestablished with stored digital identity.

21. Examples of different accounts

a. A change in the member's Navy category status, SELRES who are mobilized, volunteers for Active Duty for Special Work, serves on extended Active Duty for Training or is accepted back on a recall for indefinite Active Duty/FTS Program/or a two-year recall, may qualify for a deactivated account or EMAIL redirection. If a member has been assigned to a joint billet or a billet where NMCI/CoSC is not available, their account should be placed in a deployed status by using the EMAIL redirection tool available on the NMCI/CoSC Homeport. Examples include but are not limited to:

(1) SELRES recalled to a Navy Reserve full time billet
Example: SELRES is recalled to serve in a NAVOPSPTCEN Executive Commander billet. The gaining activity will transfer the account from the owning activity to the new activity. Deactivation or EMAIL redirection not required.
(2) SELRES recalled to a Navy active component (AC) billet. Reserve member accepts a recall to indefinite active duty. Member will be serving in the AC, therefore, the account must be transferred to the AC Navy Command. Submit a Move-Add-Change (MAC) to assign it to their Project Service Interface (PSI) code in NET. Deactivation or EMAIL redirection not required.

(3) SELRES is mobilized. Member will be serving with Navy AC, therefore, the account may be transferred to the AC Navy Command for the period of the mobilization. Submit a MAC to assign it to the new command’s PSI code in NET. No deactivation or EMAIL redirection is required. When the reserve member is demobilized, their reserve command needs to transfer the account back to the original PSI code.

(a) When a member is mobilized or transfers to another unit, the previous unit is responsible for checking the account after 90 days and ensuring the member’s account has been transferred. If the member is transferred to the Individual Ready Reserve (IRR), the account should be suspended for 90 days. The local CTR will inform a member transferring to the IRR that after 90 days the account will be permanently deactivated and their data will be permanently deleted unless the member reaffiliates with another unit. If the member transfers to a unit that does not have NMCI/CoSC, then the account should be evaluated for deactivation or EMAIL redirection.

(b) If a member is in an active drill status and also serves as a Navy civil servant or approved Navy contractor, the member will be authorized two NMCI/CoSC accounts. The primary account will be CAC-enabled while the other account will be placed on the Cryptographic Logon exceptions list.

(c) If member is transferring to a command where NMCI/CoSC is available, the gaining activity will submit an administrative MAC to transfer the account to the appropriate claimant/OU or command. Do not deactivate accounts of members transferring between commands serviced by NMCI/CoSC.

Enclosure (1)
# NMCI/CoSC Ordering Guidelines

<table>
<thead>
<tr>
<th>Echelon</th>
<th>Position</th>
<th>NMCI/CoSC Desktop</th>
<th>MobiKEY</th>
<th>BlackBerry</th>
<th>HVD</th>
<th>NMCI/CoSC Laptop</th>
<th>Wi-Fi Card / Cellular Wi-Fi</th>
</tr>
</thead>
<tbody>
<tr>
<td>II/III</td>
<td>N00</td>
<td>1</td>
<td>1A</td>
<td>1A</td>
<td>N/A</td>
<td>3</td>
<td>3 or 3A</td>
</tr>
<tr>
<td>II/III</td>
<td>N00B</td>
<td>1</td>
<td>1A</td>
<td>1A</td>
<td>N/A</td>
<td>3</td>
<td>3 or 3A</td>
</tr>
<tr>
<td>II/III</td>
<td>N01</td>
<td>1</td>
<td>1A</td>
<td>1A</td>
<td>N/A</td>
<td>3</td>
<td>3 or 3A</td>
</tr>
<tr>
<td>II/III</td>
<td>N01B</td>
<td>1</td>
<td>1A</td>
<td>1A</td>
<td>N/A</td>
<td>3</td>
<td>3 or 3A</td>
</tr>
<tr>
<td>II/III</td>
<td>N00C</td>
<td>1</td>
<td>1A</td>
<td>1A</td>
<td>N/A</td>
<td>3</td>
<td>3 or 3A</td>
</tr>
<tr>
<td>II/III</td>
<td>N00A</td>
<td>1</td>
<td>1A</td>
<td>1A</td>
<td>N/A</td>
<td>3</td>
<td>3 or 3A</td>
</tr>
<tr>
<td>II/III</td>
<td>Special Assistants</td>
<td>1</td>
<td>1A</td>
<td>1A</td>
<td>N/A</td>
<td>3</td>
<td>3 or 3A</td>
</tr>
<tr>
<td>II/III</td>
<td>Flag Assistants</td>
<td>1</td>
<td>1A</td>
<td>1A</td>
<td>N/A</td>
<td>3</td>
<td>3 or 3A</td>
</tr>
<tr>
<td>II/III</td>
<td>DCOSs</td>
<td>1</td>
<td>1A</td>
<td>1A</td>
<td>N/A</td>
<td>3</td>
<td>3 or 3A</td>
</tr>
<tr>
<td>II/III</td>
<td>FTS</td>
<td>1</td>
<td>1A</td>
<td>1A</td>
<td>N/A</td>
<td>3</td>
<td>3 or 3A</td>
</tr>
<tr>
<td>IV/V</td>
<td>Commander</td>
<td>1</td>
<td>1A</td>
<td>1A</td>
<td>N/A</td>
<td>3</td>
<td>3 or 3A</td>
</tr>
<tr>
<td>IV/V</td>
<td>CSO</td>
<td>1</td>
<td>1A</td>
<td>1A</td>
<td>N/A</td>
<td>3</td>
<td>3 or 3A</td>
</tr>
<tr>
<td>IV/V</td>
<td>Senior Enlisted Advisor</td>
<td>1</td>
<td>1A</td>
<td>1A</td>
<td>N/A</td>
<td>3</td>
<td>3 or 3A</td>
</tr>
<tr>
<td>IV/V</td>
<td>FTS</td>
<td>1</td>
<td>1A</td>
<td>1A</td>
<td>N/A</td>
<td>3</td>
<td>3 or 3A</td>
</tr>
<tr>
<td>VI</td>
<td>Commissioned Unit CO</td>
<td>1</td>
<td>1A</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td>3 or 3A</td>
</tr>
<tr>
<td>VI</td>
<td>Unit CO/OIC</td>
<td>1</td>
<td>N/A</td>
<td>N/A</td>
<td>2</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>VI</td>
<td>Unit Admin Seat</td>
<td>1</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>VI</td>
<td>SELRES</td>
<td>5</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Notes:**

1 - Members authorized a desktop are not authorized a Laptop/Wi-Fi, Cellular Wi-Fi Card or HVD.

1A - MobiKEY (for use with Desktop only) and BlackBerry require upper Echelon COS/CSO authorization.

2 - Members authorized a HVD are not authorized a Desktop, Laptop/Wi-Fi or Cellular Wi-Fi Card.

3 - Members authorized a Laptop/Wi-Fi or Cellular Wi-Fi Card are not authorized a Desktop, MobiKEY or HVD.

3A - Cellular Wi-Fi card is authorized in place of a standard Wi-Fi card when wireless connectivity is not feasible or "Access Anywhere" is required.

4 - Unit COs may choose a Blackberry only if no other mobile device has been issued (Laptop/Wi-Fi Cellular Wi-Fi Cards or HVD).

5 - SELRES to NMCI Desktop based on 18:1 Model.

6 - FTS Enlisted to NMCI Desktop based on 3:2 Model.

Figure 1-1

Enclosure (1)
CHAPTER 2
SOFTWARE AND USER PERMISSIONS

1. CAC Enabled Sites. Each SELRES member is required to maintain access to various CAC-enabled Navy sites such as Navy Reserve Homeport (NRH) and Outlook Web Access. To facilitate access to these sites from personal or non-NMCI devices, COMNAVRESFOR will disburse one CAC reader per SELRES, via chain of command.

2. SharePoint. All (ECH II-VI) reserve commands are required to maintain a private SharePoint site via NRH. Requirements are defined as follows:

   a. Landing Page, considered to be the first viewable page for each command. This page will contain:

      (1) Command name.

      (2) Announcement section.

      (3) Mission statement.

      (4) Leadership photos and biographies.

      (5) Command profile (address, hours of operation, contact phone numbers, command logo).

      (6) Hyperlinks to POM and drill weekend schedule.

      (7) Hyperlinks to site owner.

      (8) COMNAVRESFOR maintained required Awareness Logos (i.e., Sexual Assault Prevention and Response, Anti-Terrorism/Force Protection, Suicide Prevention).

   b. Each section of the Landing Page must adhere to the COMNAVRESFOR approved layout.

   c. Additional site pages are authorized as required by each command.
d. Creation of Sub Sites for lower echelon commands requires NAVRES 5300/3 (2-14) to be completed and submitted via the RCC to COMNAVRESFOR Helpdesk.

3. Site Troubleshooting. Troubleshooting SharePoint related items should be handled at the lowest echelon level as required using the IT chain of command.

4. Site Permission Management. To verify each person is assigned appropriate privileges/permissions, each command will validate its subordinate command’s assignments to site owner roles. Example: RCCs will validate NAVOPSPTCENs; NAVOPSPTCENs will validate reserve units.

   a. Community of Interest site permissions (full control) will be approved and maintained by submitting a ticket to COMNAVRESFOR’s Helpdesk. Submitted tickets must include parent site URL for which permissions are being requested.

   b. Other permissions will be maintained by local SharePoint site owners.

5. SharePoint Training. Review of SharePoint training PowerPoint presentations are required by all personnel prior to receiving permissions to author, manage or contribute site information.

   a. SharePoint site owners are required to review SharePoint Training Levels 100, 200 and Site Owner PowerPoint presentations prior to receiving full control permissions. Presentations are located at https://private.navyreserve.navy.mil/COMNAVRESFOR/N-Codes/n6/ITtraining/default.aspx

   b. Contributors are required to complete SharePoint Training Level 100 prior to receiving contribute permissions.

   c. COMNAVRESFOR will schedule additional SharePoint training bi-weekly and on a requested basis.

6. User Profile Synchronization. All Reserve Personnel requiring access to SharePoint must have a .mil or .gov EMAIL address associated to their profile.

Enclosure (1)
a. SharePoint Profiles (Display name, phone number, EMAIL address) will automatically update via the user profile Synchronization for users who maintain an NMCI EMAIL account.

b. Non-NMCI users will be required to contact COMNAVRESFOR's SharePoint Helpdesk for manual updates to their SharePoint User Profile (Display name, phone number, EMAIL address).

7. Linking .COM Sites. Linking of .COM sites/links will be allowed on SharePoint pages only if they have a mission need and those sites have been screened/reviewed for associated risks by COMNAVRESFOR N64.

8. Commercial EMAIL. Department of the Navy (DON) personnel are authorized to access commercial web-based EMAIL using DON IT resources for personal use within the limitations of reference (b).

   a. Use of commercial EMAIL for official business is only permitted when necessary to meet operational requirements in cases when DON provided EMAIL is unavailable. Each user must be endorsed by the first O-6/GS-15 in the chain of command and approved in advance by the Designated Approval Authority (DAA) responsible for specific network (or the DAA's written designee).

   b. User must follow specific guidelines defined in references (c) and (d) to ensure Controlled Unclassified Information (CUI), including Personally Identifiable Information (PII) and For Official Use Only (FOUO) is safeguarded. Commercial EMAIL cannot be authorized to transmit unencrypted CUI, to include PII. Violations of this rule must be reported to COMNAVRESFOR IAM (N64).

   c. Any records generated through use of commercial EMAIL for official business must be protected per references (e) and (f).

   d. To ensure the confidentiality, integrity, availability and security of DON IT resources and information, users shall not:

       (1) Auto-forward any EMAIL from a DON account to a commercial EMAIL account (i.e. .com, .edu, .biz).

Enclosure (1)
(2) Bypass, stress or test IA or Computer Network Defense mechanisms (firewalls, content filters, proxy servers, anti-virus programs).

(3) Introduce or use unauthorized software, firmware or hardware on any DON IT resource.

(4) Relocate or change equipment or the network connectivity of IA authority (i.e., person responsible for the overall implementation of IA at the command level).

(5) Use personally owed hardware, software, shareware or public domain software without written authorization from the local IA authority.

(6) Upload/Download executable files (e.g., .exe, .com., .vbs or .bat) onto DON IT resources without the written approval of the local IA authority.

(7) Participate in or contribute to any activity resulting in a disruption or denial of service.

(8) Write, code, compile, store, transmit, transfer or introduce malicious software, programs or code.

(9) Per reference (b), SEC 2-301, use IT resources in a way that would reflect adversely on the DON. Such uses include pornography, chain letters, unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use, violation of statute or regulation, inappropriately handled classified information and PII and other uses that are incompatible with public service.

(10) Place data onto DON IT resources possessing insufficient security controls to protect that data at the required classification (e.g., secret onto unclassified).

   e. To ensure the confidentiality, integrity, availability and security of DON IT resources and information, users shall:

   (1) Safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction or misuse.
(2) Protect CUI, to include PII and classified information to prevent unauthorized access, compromise, tampering or exploitation of the information.

(3) Protect authenticators (e.g., passwords and personal identification numbers) required for logon authentication at the same classification as the highest classification of the information accessed.

(4) Protect authentication tokens (e.g., CAC, Alternate Logon Token, Personal Identity Verification, National Security Systems tokens) at all times. Authentication tokens shall not be left unattended at any time unless properly secured.

(5) Virus check all information, programs and other files prior to uploading onto any DON IT resource.

(6) Report all security incidents including PII breaches immediately in accordance with applicable procedures.

(7) Access only data, controlled information, software, hardware and firmware for which the user is authorized access by the cognizant DON CO, has a need-to-know and has the appropriate security clearance. Assume only those roles and privileges for which the user is authorized.

(8) Observe all policies and procedures governing the secure operation and authorized use of DON information system.

(9) Digitally sign and encrypt EMAILs per reference (g).

(10) Employ sound operations security measures in accordance with DoD, DON, service and command directives.

9. Defense Connect Online. Navy-wide ashore use of Defense Connect Online (DCO) will be the standard collaboration tool for chat and web conferencing. DCO is the single designated and approved enterprise tool for Non-Classified Internet Protocol Router Network (NIPRNET) and SIPRNET web-based conferencing, instant messaging, white boarding and application sharing. DCO is the sole navy approved application to provide collaboration functions by Navy Functional Area Managers.

a. All users with online collaboration responsibilities will obtain DCO accounts and maximize use of DCO capabilities. Users must have a CAC in order to register for an account.
b. Implementation of DCO (JABBER) chat is directed to be the primary means of ashore Instant Messaging/TEXT messaging.

c. Waiver requests for alternate collaboration tools are required for commands who are unable to comply with the DCO requirement and must be approved by the Deputy Chief Information Officer Navy (DDCIO-N).
CHAPTER 3
INFORMATION TECHNOLOGY SUPPORT AND VERIFICATION

1. Continuity of Operations Plan. COMNAVRESFOR will verify functionality of the COMNAVRESFOR IT Continuity of Operations Plan (COOP) plan by exercising the COOP annually as required by reference (h). COOP dates will be advertised for command planning purposes. Upon completion of annual exercise or actual COOP, Commands are required to validate their site content for access and functionality.

2. COMNAVRESFOR Remote Site IT Support. Updates, user account maintenance, hardware installations and other IT related functions are available from COMNAVRESFOR remote site IT support. COMNAVRESFOR schedules quarterly site visits, however, commands can request site visits more frequently as required. When onsite support is not available, COMNAVRESFOR remote site IT support personnel can still provide support remotely. Remote site support personnel are prohibited from troubleshooting personal computing devices. The vast number of operating systems and hardware configurations loaded on personal computers make this function beyond the scope of IA or IT workforce. Troubleshooting systems is a personal responsibility.

3. System Authorization Access Forms. System Authorization Access (SAAR) forms are a prerequisite for access to any DoD system. Navy SAAR forms may be referred to as “SAAR-N”. SAAR Forms Sections I-III are required to be completed in full and kept on file by the local command per references (i), Chapter 5, and (j). A favorable National Agency Check with Local Agency Checks and Credit Check (NACLC) is required for unclassified network access. For military, in most cases network access may be granted if the NACLC is expired. For military, government employees and contractors, in instances where no NACLC was ever started, the NACLC must be initiated before permitting unclassified network access to personnel. If personnel have a revoked or denied NACLC status, the issues must be resolved within two years at the individual’s current command or network access should be restricted. SAAR-N Section IV will be completed as required. Commands shall retain SAAR forms for six years after user account is terminated or when no longer needed for investigative or security purposes, whichever is later.

Enclosure (1)
CHAPTER 4

NAVY OPERATIONAL SUPPORT CENTER WI-FI USAGE PROCEDURES
AND USER RESPONSIBILITIES

1. General. To promulgate guidance for Navy NAVOPSPTCEN Wi-Fi (NNWF) usage, including mandatory wireless device set-up requirements for maximum information assurance, security and overall user responsibilities. Only those wireless devices meeting the standards specified in this instruction are approved for connectivity to NNWF. The procedures and policy items contained within this document meet the requirements of reference (k).

2. Scope. These procedures and user responsibilities apply to all COMNAVRESFOR military, civilian and contract personnel assigned to locations with NNWF services installed, system maintainers and managers, all users and all wireless infrastructure devices connecting to the Wi-Fi network. User access to NNWF resources is a privilege. Responsible system management is required to maintain confidentiality, integrity and availability of information assets.

3. Bring Your Own Device. NNWF provides a “bring your own device” option to all NAVOPSPTCENs and other approved Reserve commands. Providing Wi-Fi network access to personal computers with CAC readers mitigates the challenge of limited computer seats during high-demand times. NNWF is a DoD system granted authority to operate by the Navy Network Warfare Command Operational DAA. It is completely separate and distinct from the NMCI wireless Local Area Network. All regulations pertaining to NNWF are governed by COMNAVRESFOR and is managed by the COMNAVRESFOR IT department.

4. Responsibilities

a. Reserve Force NNWF Program Manager will:

   (1) Provide NNWF program management and overall risk management.

   (2) Coordinate with Force IAM to adjudicate IA violations related to NNWF usage and make recommendations for all cases.
b. RCC N6:

(1) Report all Information Assurance violations to the Force IAM and assist in all administrative matters pertaining to NNWF.

(2) Conduct periodic site visits to inspect and ensure adherence to Force IA requirements. Inspections will include, but not limited to: user registration process, router passphrase management process, physical security of Wi-Fi equipment, user conduct in Wi-Fi spaces and signal footprint to ensure broadcast in authorized areas only.

(3) Maintain situation awareness regarding Wi-Fi use at subordinate commands.

(4) Make recommendations to COMNAVRESFOR to install new Wi-Fi networks at Reserve sites with a high demand signal for network usage or to add Wireless Access Points (WAP) to current site configurations.

c. NAVOPSPTCEN COs/Officer In Charge (OICs) will:

(1) Implement and ensure adherence to this policy. CO/OIC's direct involvement is required to ensure that security and IA is maintained.

(2) Enforce strict compliance with Wi-Fi usage policy and ensure access is denied to users who violate policy.

(3) Verify physical security of Wi-Fi system router in a secure, locked space. Do not permit tampering with system settings in any way.

(4) Make recommendations to Echelon IV to install Wi-Fi at Reserve sites with a high demand signal for network usage or to add WAP to current site configurations.

d. NAVOPSPTCEN/Reserve Site Information Assurance Officer (IAO)/IAM will:

(1) Act as designated administrator of Wi-Fi network and take responsibility for implementation of procedures for validating users and wireless devices.

Enclosure (1)
(2) Ensure WAP passphrase is strong. The passphrase shall be a minimum 14 characters, including two upper case, two special and two numeric characters. Pass phrases shall be changed no later than Thursday, prior to the first Drill Weekend of each month. NMCI laptops are authorized for changing WAP passphrases.

(3) Verify all wireless devices are configured for maximum security per Figure 4-1. Verification will be completed prior to connection to the Wi-Fi network.

(4) Ensure all Wi-Fi users are current on annual Information Assurance Annual Training (IAAT) and PII training. If delinquent, users shall not be permitted to connect to Wi-Fi.

(5) Ensure users requesting access to the Wi-Fi network complete Navy Reserve Forces NAVOPSPTCEN Wi-Fi User Agreement Forms, SD Form 815, August 2002. SD Form 815 will be reviewed annually and be retained for two years from approval of access.

(6) Maintain oversight of user registration form on SharePoint Reserve Force Wi-Fi Portal that tracks individual users to include Media Access Control (MAC) address of their personal computer. Verify users have completed registration form in its entirety.

(7) On the initial device connection to the Wi-Fi Network, verify that users have the latest version of anti-virus protection software on their personal computer. A link to a website for anti-virus software download is available on the COMNAVRESFOR N64 portal.

(8) If any user is found to be in violation of this instruction or IA procedures immediately report user to the NAVOPSPTCEN CO/Unit OIC and block the respective devices MAC address at the router.

(9) Conduct random walk-through in wireless spaces to verify proper use. Report misuse to the NAVOPSPTCEN CO/Unit OIC and ensure the user disconnects from the network.

(10) Due to specific security requirements for the Wi-Fi system, ensure physical integrity of the router and its installed parameters. Router must remain in locked and secure space. Settings shall not be modified once installed.

e. NNWF Users will:

(1) Follow the procedures and policy set forth in this instruction and the NNWF User Agreement.

(2) Ensure personal computing devices have requisite hardware installed, including a wireless adapter and CAC reader.

(3) To expedite access to Wi-Fi resources, ensure personal computing device meets the requirements of the Navy Reserve Force’s NAVOPSPTCEN Wi-Fi User Agreement forms, SD FORM 815, Aug 2002, prior to drill weekend or first use of Wi-Fi network.

(4) Complete Wi-Fi User Registration Form, via link found on the COMNAVRESFOR Wi-Fi Portal within the private CAC-enabled Sharepoint portal. Access to NNWF is strictly dependent on users having a current SAAR-N on record and completing the User Agreement form linked to this registration process.

(5) Use NNWF to connect to .mil, .gov, .edu domains and other authorized Internet sites as designated by COMNAVRESFOR. Wi-Fi is only to be utilized for accessing public-facing web sites and DoD public-facing CAC enabled Web sites.

(6) Ensure no sensitive information, including PII or "FOUO" documents are stored on personal computing devices, including personal hard drives, computer memory and temporary files.

5. Trouble Shooting Personal Devices. The NAVOPSPTCEN CO, Site OIC or local IAM/IAO or IT workforce personnel are prohibited from troubleshooting personal computing devices. The vast number of operating systems and hardware configurations loaded on personal computers make this function beyond the scope of IA or IT workforce.

a. Troubleshooting systems is a personal responsibility.
b. Users bear all risk associated with use of NNWF network. The government is not liable for any damage or loss incurred as a result of network use.

6. **Enforcement.** A user found to have violated this policy will have their NNWF privileges revoked and may be subject to disciplinary action. Users may be re-instated at the Force IAM discretion. Level of re-instating authority depends on nature and scope of violation. Example violations warranting access denial include:

   a. Improper use of Wi-Fi, as defined in the User Agreement.

   b. Visiting sites that would bring discredit to Naval Service (e.g. gambling sites, pornography).

   c. User does not have a current NMCI account.

   d. User deficient in annual IAAT or PII training.

   e. Other reasons as determined by site Commander, RCC, Echelon IV IAO/IAM or Force IAM.
Before initially being approved for connecting to the NAVOPSPTCEN Wi-Fi Network, the following actions must be completed:

- Verify IAAT and PII annual training requirements are within periodicity.

- Register as a new user to the Wi-Fi network on Wi-Fi website, accessible by link on NRH Private Portal, COMNAVRESFOR, N6 homepage. Ensure your MAC address and drill site location is captured and accurate.

- Sign and date NAVOPSPTCEN Wi-Fi User Agreement form.

- Install and test CAC reader on your personal laptop.


- Enable firewall.

- Print out confirmation of registration.

- Receive passphrase from designated command Information Awareness Workforce representative.

After initial approval for Wi-Fi access is granted, users are responsible for maintaining virus updates and ensuring that the firewall is enabled prior to network access per the user agreement.
APPENDIX A
ACRONYMS AND DEFINITIONS

The following is a list of the current acronyms and definitions referenced throughout this instruction.

Anti-Virus Software. Software designed to prevent, detect and remove malware, including but not limited to computer viruses, computer worms, Trojan horses, spyware and adware.

Authority To Operate. An Authority To Operate (ATO) is the formal approval (accreditation) to operate a system, which is granted by the DAA. Once granted, an ATO is good for three years.

Common Access Card. A U.S. DoD issued smart card for multifactor authentication to networks and information systems. CACs are issued as standard identification for active-duty military personnel, reserve personnel, civilian employees, non-DoD government employees, state employees of the National Guard and eligible contractor personnel. In addition to its use as an identification card, a CAC is required for access to government buildings and computer networks.

CAC Reader. A physical device used as a communications medium between the CAC and a host (e.g., a computer, a point of sale terminal) or a mobile telephone.

Media Access Control Address. A unique identifier assigned to network interfaces and devices for communications on the physical network segment.

Office of the Designated Approving Authority. Provides centralized management and de-centralized execution of the certification and accreditation (C&A) process for all DoD information systems. The Office of the DAA is accountable for timely, consistent policy implementation and C&A determinations with the DoD.

Passphrase. A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.
Personally Identifiable Information. Refers to information that can be used to uniquely identify, contact or locate a single person or can be used with other sources to uniquely identify a single individual. Includes name, birth dates, Social Security Numbers, rank, address, phone number, etc.

Physical Security. Describes measures designed to deny access to unauthorized personnel (including attackers or even accidental intruders) from physically accessing a building, facility, resource or stored information.

Wi-Fi. A branded standard for wirelessly connecting electronic devices. A Wi-Fi device, such as a personal computer, can connect to the Internet via a wireless network access point.
APPENDIX B

FORMS AND UNIFORM RESOURCE LOCATOR AVAILABILITY

The following Web sites are an additional source for forms:

SharePoint Form: Title and URL to be added by Command Services.

Navy Reserve Forces NAVOPSPTCEN Wi-Fi User Agreement Forms, SD Form 815, August 2002:
https://private.navyreserve.navy.mil/cnrfc/n-codes/n6/Wi-Fi/Shared%20Documents/Wi-Fi_Encl1.doc

Navy Reserve Forces NAVOPSPTCEN Wi-Fi User Agreement (SD Form 815, Aug 2002):
http://www.dtic.mil/whs/directives/infromgt/forms/index.htm

Anti-Virus Software Download: